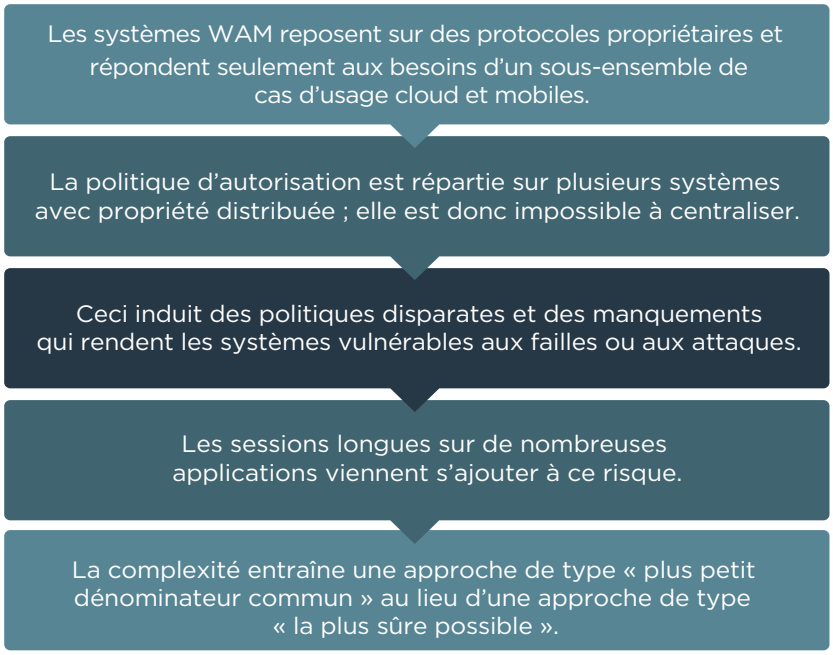
GUIDE A L'USAGE DES RESPONSABLES SECURITE : SECURITE DES ACCES

Comme de nombreux responsables sécurité, vous vous trouvez peut-être dans les affres de la transformation numérique. Vos utilisateurs et vos applications dépassent souvent votre périmètre de sécurité initial et votre tâche consiste désormais à sécuriser votre entreprise numérique contre des menaces de sécurité plus nombreuses. Le tout sans nuire à la productivité ni à la croissance.

Vous pouvez envisager d'utiliser votre système existant de gestion des accès web (WAM), mais cette solution sera, au mieux, assez compliquée pour gérer les mesures de sécurité modernes, et au pire, vraiment risquée.

Inadaptés aux défis actuels, les systèmes WAM ne prennent pas en charge la migration d'applications vers le cloud et ne savent pas bien gérer les applications mobiles et les API. Vous pouvez essayer d'ajouter des modules complémentaires, mais cela est complexe, nécessite beaucoup de ressources et crée un effet domino qui laisse votre entreprise vulnérable.

Problèmes liés aux systèmes WAM pour une sécurité moderne



Mais il n'est pas possible non plus de rester les bras croisés. Vous avez besoin d'un solution conçue pour répondre aux défis actuels. Une solution qui fournissent les éléments suivants :

- Un accès sécurisé, centralisé et basé sur des règles pour tous les utilisateurs, à toutes les applications, quel que soit leur type ou leur emplacement (cloud public ou privé, local, entreprise, tiers, mobile).
- Une gestion des accès en fonction du contexte qui s'adapte à l'utilisateur et effectue une vérification continue de ce dernier, de l'appareil et des données d'application, notamment localisation, réseau et statut de l'appareil.
- Un contrôle centralisé des données d'identité avec gouvernance des données basée sur des règles, gestion de la confidentialité et du consentement, et sécurité des données d'identité de bout en bout.
- Une plate-forme extensible avec prise en charge complète des standards IAM modernes pour les cas d'usage employés, partenaires et clients.

Autrement dit, pour sécuriser votre entreprise moderne, vous avez besoin d'une solution moderne de sécurité des accès.

01

LA MODERNITÉ PAR LES IDENTITÉS

En matière de sécurité et d'octroi des accès au delà du pare-feu, l'identité constitue la passerelle. En sécurisant vos applications web et vos API avec des standards d'identité aboutis, ainsi qu'avec les tout derniers protocoles d'authentification et d'autorisation, vous pouvez offrir aux bonnes personnes un accès aux contenus adéquats, en toute sécurité et en toute fluidité.

Une gestion moderne des accès nécessite une approche en trois volets qui offre aux utilisateurs un accès sécurisé à toutes les applications et ressources :

1. **Single Sign-on (SSO) :** remplace tous ces mots de passe par un ensemble unique d'identifiants d'entreprise et une expérience d'authentification cohérente.
2. **Authentification multi-facteurs (MFA) :** ajoute une autre couche de sécurité en plus des mots de passe ; incontournable pour l'entreprise numérique.
3. **Sécurité des accès :** centralise le contrôle d'accès via une couche de sécurité basée sur les règles pour toutes les applications web et mobiles ainsi que les API.

Une sécurité moderne des accès vous permet de former un point d'accès central pour vérifier qui a accès à quoi et pendant combien de temps. Vous pouvez déployer vos applications en local, dans un cloud privé ou public, tout en assurant le même niveau de gestion des accès et des identités dans les trois cas. Et vous pouvez le faire rapidement pour protéger les nouveaux systèmes, en accélérant la transformation numérique.

Il est naturel de vouloir exploiter votre système existant, mais les systèmes WAM, qui sont antérieurs aux applications cloud et mobiles, sont censés protéger les ressources web internes hébergées dans les centres de données de l'entreprise. En combinant un système WAM existant avec des passerelles d'API, l'intégration est limitée, sans parler de la complexité du déploiement et de la gestion. Il vous reste alors des produits lourds mais fragiles qui nécessitent des services d'intégration système exigeants pour de simples installations et mises à jour. Sans oublier une approche de sécurité porteuse de risque, dans le meilleur des cas.

Résultat : se reposer sur un système existant pour remplir une mission pour laquelle il n'est pas conçu freine la croissance et augmente les coûts, les casse-têtes et votre vulnérabilité face aux attaques.

02

LA STANDARDISATION PAR LES STANDARDS

Aujourd'hui, la plupart des entreprises utilisent l'authentification et l'autorisation par mot de passe pour les API. En l'absence de systèmes d'identités standardisés, il s'agit d'une interaction simple et hautement sécurisée :

UTILISATEUR » APPL. :	Bonjour, je voudrais voir mes données.
APPL. » UTILISATEUR :	Veuillez vous identifier avec votre nom d'utilisateur et votre mot de passe.
APPL. » API :	Bonjour, j'ai besoin d'accéder au Service A, voici le nom d'utilisateur et le mot de passe.
API » APPL. :	OK, voici le Service A.
APPL. » UTILISATEUR :	Voici les données demandées.

Le principe ci-dessus s'applique, que le service auquel accède l'utilisateur soit un site de réseau social ou une application cloud ou que l'appareil utilisé soit un ordinateur de bureau, un ordinateur portable, une tablette ou un téléphone. Il est essentiel de sécuriser l'accès aux API tant pour les applications web que mobiles. Il ne s'agit évidemment pas d'une solution sécurisée pour contrôler les accès et ne fournit aucun niveau d'accès.

Le protocole OAuth 2.0 apporte une réponse en autorisant le client à formuler officiellement une demande d'accès à une ressource (une API) via un jeton d'accès précédemment émis par un serveur d'autorisation. Le protocole OAuth spécifie trois rôles lors de ce processus :

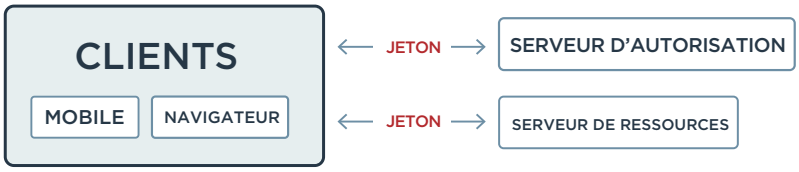


Figure 1 : Le protocole OAuth 2.0 autorise le client à formuler officiellement une demande d'accès à une API via un jeton émis par un serveur d'autorisation.

CLIENT : habituellement une application (web ou mobile) qui souhaite accéder à une API particulière.
SERVEUR D'AUTORISATION : un serveur qui émet des jetons d'accès et les actualise de la part du serveur de ressources.
SERVEUR DE RESSOURCES : un serveur qui héberge et protège les ressources et les rend disponibles auprès des clients correctement authentifiés et autorisés.

Comme le montre la Figure 1, une solution moderne de sécurité des accès qui prend en charge OAuth fournit une façon sécurisée d'authentifier un utilisateur, de demander le consentement et de fournir un contrôle sur le niveau d'autorisation, ce qui est fondamental pour gérer un accès sécurisé à l'entreprise d'aujourd'hui.

En savoir plus ? Lisez Essential OAuth Primer.

03

CONTRÔLE D'ACCÈS DYNAMIQUE AU NIVEAU DE LA PAGE

Aujourd'hui, la plupart des entreprises ont intégré un certain niveau d'autorisation dans les applications, ce qui peut compliquer le respect des règles, en augmenter le coût et le temps qui leur est consacré. Pour gérer les autorisations, il est plus judicieux d'utiliser une seule couche de contrôle qui détermine la politique d'accès pour chaque application et page d'application.

Supposons qu'il s'agisse d'une application de vente avec une page ou une section réservée aux membres privilèges. Lorsqu'un utilisateur clique pour naviguer jusqu'à cette page, vous devez déterminer s'il peut ou non bénéficier de l'accès.
Une solution moderne de sécurité des accès protège toutes les URL avec un proxy/passerelle qui exécute les règles.
Ces règles ressemblent habituellement à ceci :

- Vérifier si l'utilisateur s'est déjà connecté (s'est authentifié).
- Exiger de l'utilisateur qu'il s'authentifie s'il n'est pas déjà connecté.
- Vérifier les attributs de l'utilisateur une fois qu'il est authentifié afin de déterminer si les règles l'autorise à accéder à la page.
- Pour les pages à contenu sensible, exiger de l'utilisateur (si autorisé) à s'authentifier par étapes via l'authentification multi-facteurs ou autre mécanisme.
- Afficher la page.

Aujourd'hui, les solutions de sécurité des accès vous permettent d'appliquer des règles de manière centrale à plusieurs pages ou applications.
Si vous devez modifier les règles d'accès à une page, il n'est pas nécessaire de modifier l'application.

04

ACCÉLÉREZ VOTRE MIGRATION CLOUD

Une solution moderne de sécurité des accès vous permet d'assurer un accès sécurisé aux applications, mais aussi d'accélérer votre migration des applications existantes vers des environnements cloud (comme Amazon Web Services).

Grâce à une architecture légère basée sur un proxy et des règles d'accès à gestion centralisée, vous pouvez appliquer une politique de sécurité pour les applications qui étaient précédemment gérées par les systèmes WAM, comme CA Siteminder ou Oracle Access Manager. Une fois les applications migrées vers le nouveau système, vous pouvez les déplacer vers tout environnement, facilement, à tout moment.

Voulez-vous ce type de solution réactive, flexible et légère pour répondre à vos défis de sécurité actuels ?

Assurer un accès sécurisé est un défi plus réel que jamais. Inutile donc de vous compliquer la tâche. Les identités vous donnent la clé pour autoriser les bonnes personnes à accéder aux contenus adéquats, en toute fluidité et en toute sécurité.

Vous voulez en savoir plus sur l'utilisation des identités pour sécuriser votre entreprise ? Lisez notre Ultimate Guide consacré à la gestion moderne des accès.